

## IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A removable physical media bearing a computer program operable to control a computer to detect[[ing]] malware by performing the steps of:
  - booting said computer with a non-installed operating system read from said removable physical media instead of an installed operating system stored on said computer;
  - loading network support code for said computer read from said removable physical media;
  - downloading from a remote computer one or more malware detection files;
  - [[and]]
  - performing malware detection upon said computer using said one or more malware detection files; and
  - establishing a secure network connection to said remote computer;
  - wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection;
  - wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer.
2. (Original) A removable physical media as claimed in claim 1, wherein said one or more malware detection files include at least one of:
  - malware definition data containing data characteristic of malware to be detected;
  - a malware detecting engine operable to control said computer to perform said malware detection;
  - a malware application shell; and
  - malware detection option settings operable to configure optional settings of said malware detection.

3. (Original) A removable physical media as claimed in claim 1, wherein said steps further comprise loading security management code operable to control said downloading.

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Original) A removable physical media as claimed in claim 1, wherein said removable physical media is one of:

- an optical disk;
- a floppy disk;
- a memory card; and
- a removable disk drive.

8. (Original) A removable physical media as claimed in claim 1, wherein malware to be detected includes one or more of:

- a computer virus;
- a computer Trojan;
- a computer worm;
- a banned computer application;
- a data file associated with a malware file; and
- configuration settings of said computer associated with a malware file.

9. (Currently Amended) A method of detecting malware upon a computer, said method comprising[[ the steps of]]:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files;  
[[and]]

performing malware detection upon said computer using said one or more malware detection files; and

establishing a secure network connection to said remote computer;  
wherein a firewall disposed between said computer and said remote computer is  
operable to block a connection between said computer and said remote computer other  
than said secure network connection;

wherein said network support code is used to enable said computer to establish  
said secure network connection via said firewall to said remote computer.

10. (Original) A method as claimed in claim 9, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;  
a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

11. (Original) A method as claimed in claim 9, comprising loading security management code operable to control said downloading.

12. (Cancelled)

13. (Cancelled)

14. (Cancelled)

15. (Original) A method as claimed in claim 9, wherein said removable physical media is one of:

- an optical disk;
- a floppy disk;
- a memory card; and
- a removable disk drive.

16. (Original) A method as claimed in claim 9, wherein malware to be detected includes one or more of:

- a computer virus;
- a computer Trojan;
- a computer worm;
- a banned computer application;
- a data file associated with a malware file; and
- configuration settings of said computer associated with a malware file.

17. (Currently Amended) A computer operable to detect malware upon said computer, said computer comprising a processor configured to [[by]] perform[[ing]] the steps of:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files;

[[and]]

performing malware detection upon said computer using said one or more malware detection files; and

establishing a secure network connection to said remote computer;

wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection;

wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer

18. (Original) A computer as claimed in claim 17, wherein said one or more malware detection files include at least one of:

- malware definition data containing data characteristic of malware to be detected;
- a malware detecting engine operable to control said computer to perform said malware detection;
- a malware application shell; and
- malware detection option settings operable to configure optional settings of said malware detection.

19. (Original) A computer as claimed in claim 17, wherein said steps further comprise loading security management code operable to control said downloading.

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Original) A computer as claimed in claim 17, wherein said removable physical media is one of:

- an optical disk;
- a floppy disk;
- a memory card; and
- a removable disk drive.

24. (Original) A computer as claimed in claim 17, wherein malware to be detected includes one or more of:

- a computer virus;
- a computer Trojan;
- a computer worm;
- a banned computer application;
- a data file associated with a malware file; and
- configuration settings of said computer associated with a malware file.

25. (Currently Amended) A server computer connected by a network link to a computer detecting malware upon said computer, said server computer comprising a processor configured to [[by]] perform[[ing]] the steps of:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a server computer establishing a secure network connection to said computer; and

loading one or more malware detection files to said computer; [[ and]]

performing malware detection upon said computer using said one or more malware detection files;

wherein a firewall disposed between said computer and said server computer is operable to block a connection between said computer and said server computer other than said secure network connection;

wherein said computer is booted with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

wherein network support code is loaded for said computer read from said removable physical media;